UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,475	03/30/2004	Hiroshi Suzuki	16869N-111600US	7769

20350 7590 01/25/2007		EXAMINER
TOWNSEND AND TOWNSEND AND CREW, LLP		DILLON, SAMUEL A
TWO EMBARCADERO CENTER		
EIGHTH FLOOR	ART UNIT	PAPER NUMBER
SAN FRANCISCO, CA 94111-3834	2185	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/814,475	SUZUKI ET AL.
	Examiner	Art Unit	
	Sam Dillon	2185	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>12 December 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-20</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-20</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>30 March 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

        1.☒ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948).

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   The Examiner acknowledges the applicant's submission of the amendment dated

December 12, 2006. Per the amendment, Claims 1, 2, 9, 11 and 15 have been amended.

2.   The instant application having Application No. 10/814,475 has a total of 20 claims

pending in the application; there are 5 independent claims and 15 dependent claims, all of

which are ready for examination by the examiner.

I. RESPONSE TO AMENDMENT(S) / ARGUMENT(S)

3.   In response to the amendment, the 35 U.S.C. 112 first paragraph rejections of **Claims**

16-19 as stated in the previous action are **withdrawn**.

4.   Applicant's arguments *(see page 11 lines 11-13 of the response dated Dec. 12, 2006)*

with respect to the 35 U.S.C. 102(b) rejections of **Claims 1-4, 6, 9-11 and 15** and additionally in

respect to the 35 U.S.C. 103(a) rejections of **Claims 5, 7-8, 12-14 and 16-20** have been fully

considered and are **persuasive**, but are moot in view of the new ground(s) of rejection, as

described below.

II. REJECTIONS BASED ON PRIOR ART

Claim Rejections - 35 USC ' 103 – Hubis, McIlroy and Feiertag

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art
> are such that the subject matter as a whole would have been obvious at the time the invention was made to
> a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

6.   **Claims 1-4, 6, 9-11 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable

over Hubis et al *(US Patent Number 6,343,324)* in view of McIlroy et al. *("Multilevel Security in*

the UNIX Tradition") and Feiertag et al. *("Proving Multilevel Security of a System Design").*

7.   As per **Claim 1**, Hubis discloses an input/output management system for managing input

or output from or to a disk device *(Hubis, disk drive storage array, column 3 lines 62-65)*

connected to a computer *(host 1, Figure 2A)*, comprising:

a connection information definition block *(NURAM 182, Figure 2A)* in which the

relationship of logical connection *(port mapping table entry 190, Figure 2B-3)* between

said computer and a logical volume *(logical volume, column 10 line 33)* included in said

disk device or a logical area *(logical volume, column 10 line 33)* in a logical volume

(physical disc drive, column 10 line 32) is defined; and

an input/output execution control block *(processor 180, Figure 2A)* that controls,

based on the definition, whether said computer can access a logical volume included in

said disk device or a logical area in a logical volume *(column 4 lines 6-8)*.

Hubis does not disclose wherein said connection information definition block includes a

logical volume connection information specification division in which a connected state value

concerning the connection of said computer is specified in relation to each logical volume

included in said disk device or each logical area in each logical volume included in said disk

device, said connected state value ranging between a minimum value and a maximum value,

said maximum value signifying that said computer is fully connected, said minimum value

signifying that said computer is fully disconnected, an intermediate value between said

maximum value and said minimum value signifying a conditionally connected state for said

computer.

McIlroy discloses a connected state value *(ceiling, section 2, paragraph 1 line 3)*

concerning the connection of said computer *(process. Section 2, paragraph 1 line 3)* is specified

in relation to each logical volume *(file system, section 2, paragraph 1 line 3)*, said connected

state value ranging between a minimum value and a maximum value *(section 2, paragraph 2*

line 1), said maximum value *(symbol "yes", section 2, paragraph 2 line 2)* signifying that said

computer is fully connected, said minimum value *(symbol "no", section 2, paragraph 2 lines 3-4)*

signifying that said computer is fully disconnected, an intermediate value *(element of a*

mathematical lattice, section 2, paragraph 2 line 1) between said maximum value and said

minimum value signifying a conditionally connected state *(when a process label has a higher*

privilege than a storage label the communication may proceed, otherwise it will not, section 1,

paragraph 2 lines 2-3) for said computer.

Hubis and McIlroy are analogous art in that they both deal with the Unix operating

system *(see Hubis, column 1 lines 41-43, and McIlroy, section 1, paragraph 1 line 1)* and

validating authorization to access files *(see Hubis, column 3 lines 52-59, and McIlroy, section 1,*

paragraph 2 lines 1-2). At the time of the invention it would have been obvious to one having

ordinary skill in the art to implement McIlroy's secure system by adding labels to Hubis' port

mapping table.

The motivation for doing so would have been that the McIlroy's system provides sound,

practical security *(abstract, lines 3-5)* and uses security labels to classify information for

purposes of privacy and integrity *(abstract, lines 5-7)*.

Therefore, it would have been obvious at the time of the invention to implement McIlroy's

security labels on Hubis' volume management system for the benefit of practical security and for

purposes of privacy and integrity.

Hubis and McIlroy disclose a connected state value having an attribute that is used to determine security permissions *(see above)*. Additionally, McIlroy discloses that a label is either a mathematical element or one of two special symbols, each implying either being completely accessible or completely inaccessible. Though it is possible to conceive of the data structure storing the mathematical element or special symbols being a numerical value, McIlroy does not *expressly* disclose the label being a numerical value. Therefore, Hubis and McIlroy do not *expressly* disclose the connected state being a numerical value.

Feiertag discloses an attribute used to determine security permissions being a numerical value *(Feiertag, L is the set of security levels of a system, and "<" is a relation that orders the set L, which can be seen as the functionally equivalent to a set of integers, page 58 right hand column)*.

Hubis, McIlroy and Feiertag are analogous art in that they deal with multilevel computer security. At the time of the invention it would have been obvious to utilize the formal model described in Feiertag to guarantee McIlroy's multilevel security system's correctness, which would inherently include forcing McIlroy's label to be a single element from an ordered set of security clearance elements.

The motivation for doing so would have been that the Bell and LaPadula model is very simple and allows the designer to verify easily that the definition is consistent with intuitive understanding of multilevel security *(Feiertag, Conclusions, page 63)*.

Therefore, it would have been obvious to modify Hubis and McIlroy's system to fit into Feiertag's formal verification scheme by making the label a numerical value for the benefit of simplicity of design and ease of design, to obtain the invention of Claim 1.

8.   As per **Claim 2**, Hubis discloses an input/output management system for managing input or output from or to a disk device *(disk drive storage array, column 3 lines 62-65)* connected to a

plurality of computers *(plurality of computers, column 4 line 3 and host 1 through M, Figure 2A)*,

comprising:

a connection information definition block *(NURAM 182, Figure 2A)* in which the

relationship of logical connection *(port mapping table 190, Figure 2A)* between each of

said computers and a logical volume *(storage volume 108, column 4 line 48 and logical*

volume 1, Figure 2A) included in said disk device or a logical area *(logical volume,*

column 10 line 33) in a logical volume *(physical disc drive, column 10 line 32)* is defined

using computer identification information *(unique identifier, column 4 line 5)*; and

an input/output execution control block *(processor 180, Figure 2A)* that controls,

based on the definition, whether each of said computers can access a logical volume

included in said disk device or a logical area in a logical volume *(column 4 lines 6-8)*.

Hubis does not disclose wherein said connection information definition block includes a

logical volume connection information specification division in which a connected state value

concerning the connection of said computer is specified in relation to each logical volume

included in said disk device or each logical area in each logical volume included in said disk

device, said connected state value ranging between a minimum value and a maximum value,

said maximum value signifying that said computer is fully connected, said minimum value

signifying that said computer is fully disconnected, an intermediate value between said

maximum value and said minimum value signifying a conditionally connected state for said

computer.

McIlroy discloses a connected state value *(ceiling, section 2, paragraph 1 line 3)*

concerning the connection of said computer *(process. Section 2, paragraph 1 line 3)* is specified

in relation to each logical volume *(file system, section 2, paragraph 1 line 3)*, said connected

state value ranging between a minimum value and a maximum value *(section 2, paragraph 2*

line 1), said maximum value *(symbol "yes", section 2, paragraph 2 line 2)* signifying that said

computer is fully connected, said minimum value *(symbol "no", section 2, paragraph 2 lines 3-4)*

signifying that said computer is fully disconnected, an intermediate value *(element of a*

mathematical lattice, section 2, paragraph 2 line 1) between said maximum value and said

minimum value signifying a conditionally connected state *(when a process label has a higher*

privilege than a storage label the communication may proceed, otherwise it will not, section 1,

paragraph 2 lines 2-3) for said computer.

   Hubis and McIlroy are analogous art in that they both deal with the Unix operating

system *(see Hubis, column 1 lines 41-43, and McIlroy, section 1, paragraph 1 line 1)* and

validating authorization to access files *(see Hubis, column 3 lines 52-59, and McIlroy, section 1,*

paragraph 2 lines 1-2). At the time of the invention it would have been obvious to one having

ordinary skill in the art to implement McIlroy's secure system by adding labels to Hubis' port

mapping table.

   The motivation for doing so would have been that the McIlroy's system provides sound,

practical security *(abstract, lines 3-5)* and uses security labels to classify information for

purposes of privacy and integrity *(abstract, lines 5-7)*.

   Therefore, it would have been obvious at the time of the invention to implement McIlroy's

security labels on Hubis' volume management system for the benefit of practical security and for

purposes of privacy and integrity.

   Hubis and McIlroy disclose a connected state value having an attribute that is used to

determine security permissions *(see above)*. Additionally, McIlroy discloses that a label is either

a mathematical element or one of two special symbols, each implying either being completely

accessible or completely inaccessible. Though it is possible to conceive of the data structure

storing the mathematical element or special symbols being a numerical value, McIlroy does not

expressly disclose the label being a numerical value. Therefore, Hubis and McIlroy do not

expressly disclose the connected state being a numerical value.

Feiertag discloses an attribute used to determine security permissions being a numerical

value *(Feiertag, L is the set of security levels of a system, and "<" is a relation that orders the*

set L, which can be seen as the functionally equivalent to a set of integers, page 58 right hand

column).

Hubis, McIlroy and Feiertag are analogous art in that they deal with multilevel computer

security. At the time of the invention it would have been obvious to utilize the formal model

described in Feiertag to guarantee McIlroy's multilevel security system's correctness, which

would inherently include forcing McIlroy's label to be a single element from an ordered set of

security clearance elements.

The motivation for doing so would have been that the Bell and LaPadula model is very

simple and allows the designer to verify easily that the definition is consistent with intuitive

understanding of multilevel security *(Feiertag, Conclusions, page 63)*.

Therefore, it would have been obvious to modify Hubis and McIlroy's system to fit into

Feiertag's formal verification scheme by making the label a numerical value for the benefit of

simplicity of design and ease of design, to obtain the invention of Claim 2.

9.   As per **Claim 3**, Hubis, McIlroy and Feiertag disclose an input/output management

system according to Claim 1, wherein said connection information definition block comprises:

a computer identification information definition division *(host computer ID map*

data structure, column 4 lines 10-11) in which physical identification information *(host*

computer ID, column 4 line 10) that uniquely indicates said computer connected to said

disk device is defined.

10.   As per **Claim 4**, Hubis, McIlroy and Feiertag disclose an input/output management

system for managing input or output from or to a disk device connected to a computer according

to Claim 1, wherein said connection information definition block comprises:

       a computer identification information definition division *(port mapping table 190,*

       Figure 2B-3) in which the relationship of logical connection *(port mapping table entry*

       191, Figure 2B-3) between said computer and a logical area in a logical volume included

       in said disk device is defined using computer identification information *(host index 151,*

       Figure 2B-3).

11.   As per **Claim 6**, Hubis, McIlroy and Feiertag disclose an input/output management

system according to Claim 1, wherein said connection information definition block comprises:

       a computer identification information definition division *(port mapping table 190,*

       Figure 2B-3) in which the relationship of logical connection *(port mapping table entry*

       191, Figure 2B-3) between said computer and a logical volume included in said disk

       device is defined using port numbers *(i/o processor number column in port mapping*

       table, Figure 2B-3) assigned to the ports of said disk device connected to said computer

       (port 114-1 through port 114-M in Figure 2A).

12.   As per **Claim 9**, Hubis discloses an input/output management method for managing

input or output from or to a disk device *(disk drive storage array, column 3 lines 62-65)*

connected to a computer *(host 1, Figure 2A)*, comprising the steps of:

       defining the relationship of logical connection *(NURAM data structures 182,*

       Figure 2A) between said computer and a logical volume *(logical volume, column 10 line*

       33) included in said disk device or a logical area *(logical volume, column 10 line 33)* in a

       logical volume *(physical disc drive, column 10 line 32)*; and

controlling, based on the definition, whether said computer can access a logical

volume included in said disk device or a logical area a logical volume *(col. 4 lines 6-8)*.

Hubis does not disclose wherein said connection information definition block includes a

logical volume connection information specification division in which a connected state value

concerning the connection of said computer is specified in relation to each logical volume

included in said disk device or each logical area in each logical volume included in said disk

device, said connected state value ranging between a minimum value and a maximum value,

said maximum value signifying that said computer is fully connected, said minimum value

signifying that said computer is fully disconnected, an intermediate value between said

maximum value and said minimum value signifying a conditionally connected state for said

computer.

McIlroy discloses a connected state value *(ceiling, section 2, paragraph 1 line 3)*

concerning the connection of said computer *(process. Section 2, paragraph 1 line 3)* is specified

in relation to each logical volume *(file system, section 2, paragraph 1 line 3)*, said connected

state value ranging between a minimum value and a maximum value *(section 2, paragraph 2*

line 1), said maximum value *(symbol "yes", section 2, paragraph 2 line 2)* signifying that said

computer is fully connected, said minimum value *(symbol "no", section 2, paragraph 2 lines 3-4)*

signifying that said computer is fully disconnected, an intermediate value *(element of a*

mathematical lattice, section 2, paragraph 2 line 1) between said maximum value and said

minimum value signifying a conditionally connected state *(when a process label has a higher*

privilege than a storage label the communication may proceed, otherwise it will not, section 1,

paragraph 2 lines 2-3) for said computer.

Hubis and McIlroy are analogous art in that they both deal with the Unix operating

system *(see Hubis, column 1 lines 41-43, and McIlroy, section 1, paragraph 1 line 1)* and

validating authorization to access files *(see Hubis, column 3 lines 52-59, and McIlroy, section 1, paragraph 2 lines 1-2)*. At the time of the invention it would have been obvious to one having ordinary skill in the art to implement McIlroy's secure system by adding labels to Hubis' port mapping table.

The motivation for doing so would have been that the McIlroy's system provides sound, practical security *(abstract, lines 3-5)* and uses security labels to classify information for purposes of privacy and integrity *(abstract, lines 5-7)*.

Therefore, it would have been obvious at the time of the invention to implement McIlroy's security labels on Hubis' volume management system for the benefit of practical security and for purposes of privacy and integrity.

Hubis and McIlroy disclose a connected state value having an attribute that is used to determine security permissions *(see above)*. Additionally, McIlroy discloses that a label is either a mathematical element or one of two special symbols, each implying either being completely accessible or completely inaccessible. Though it is possible to conceive of the data structure storing the mathematical element or special symbols being a numerical value, McIlroy does not *expressly* disclose the label being a numerical value. Therefore, Hubis and McIlroy do not *expressly* disclose the connected state being a numerical value.

Feiertag discloses an attribute used to determine security permissions being a numerical value *(Feiertag, L is the set of security levels of a system, and "<" is a relation that orders the set L, which can be seen as the functionally equivalent to a set of integers, page 58 right hand column)*.

Hubis, McIlroy and Feiertag are analogous art in that they deal with multilevel computer security. At the time of the invention it would have been obvious to utilize the formal model described in Feiertag to guarantee McIlroy's multilevel security system's correctness, which

would inherently include forcing McIlroy's label to be a single element from an ordered set of security clearance elements.

The motivation for doing so would have been that the Bell and LaPadula model is very simple and allows the designer to verify easily that the definition is consistent with intuitive understanding of multilevel security (Feiertag, Conclusions, page 63).

Therefore, it would have been obvious to modify Hubis and McIlroy's system to fit into Feiertag's formal verification scheme by making the label a numerical value for the benefit of simplicity of design and ease of design, to obtain the invention of Claim 9.

13.   As per **Claim 10**, Hubis, McIlroy and Feiertag disclose an input/output management method according to Claim 9, wherein

>   the definition of the relationship of connection contains physical identification information (host world wide name list 153, Figure 2B-1) that uniquely indicates said computer connected to said disk device.

14.   As per **Claim 11**, Hubis discloses an input/output management method for managing input or output from or to a disk device (disk drive storage array, column 3 lines 62-65) connected to a computer (host 1, Figure 2A), comprising the steps of:

>   defining, based on computer identification information (host world wide name list 153, Figure 2B-1) and logical volume connection information (volume permission table 194, Figure 2B-3), the relationship of logical connection (port mapping table 190, Figure 2B-3) between said computer and a logical volume (logical volume, column 10 line 33) included in said disk device or a logical area (logical volume, column 10 line 33) in a logical volume (physical disc drive, column 10 line 32); and

>   controlling, based on the definition, whether said computer can access a logical area in a logical volume included in said disk device (column 4 lines 6-8).

Hubis does not disclose wherein said connection information definition block includes a logical volume connection information specification division in which a connected state value concerning the connection of said computer is specified in relation to each logical volume included in said disk device or each logical area in each logical volume included in said disk device, said connected state value ranging between a minimum value and a maximum value, said maximum value signifying that said computer is fully connected, said minimum value signifying that said computer is fully disconnected, an intermediate value between said maximum value and said minimum value signifying a conditionally connected state for said computer.

McIlroy discloses a connected state value *(ceiling, section 2, paragraph 1 line 3)* concerning the connection of said computer *(process. Section 2, paragraph 1 line 3)* is specified in relation to each logical volume *(file system, section 2, paragraph 1 line 3)*, said connected state value ranging between a minimum value and a maximum value *(section 2, paragraph 2 line 1)*, said maximum value *(symbol "yes", section 2, paragraph 2 line 2)* signifying that said computer is fully connected, said minimum value *(symbol "no", section 2, paragraph 2 lines 3-4)* signifying that said computer is fully disconnected, an intermediate value *(element of a mathematical lattice, section 2, paragraph 2 line 1)* between said maximum value and said minimum value signifying a conditionally connected state *(when a process label has a higher privilege than a storage label the communication may proceed, otherwise it will not, section 1, paragraph 2 lines 2-3)* for said computer.

Hubis and McIlroy are analogous art in that they both deal with the Unix operating system *(see Hubis, column 1 lines 41-43, and McIlroy, section 1, paragraph 1 line 1)* and validating authorization to access files *(see Hubis, column 3 lines 52-59, and McIlroy, section 1, paragraph 2 lines 1-2)*. At the time of the invention it would have been obvious to one having

ordinary skill in the art to implement McIlroy's secure system by adding labels to Hubis' port mapping table.

The motivation for doing so would have been that the McIlroy's system provides sound, practical security *(abstract, lines 3-5)* and uses security labels to classify information for purposes of privacy and integrity *(abstract, lines 5-7)*.

Therefore, it would have been obvious at the time of the invention to implement McIlroy's security labels on Hubis' volume management system for the benefit of practical security and for purposes of privacy and integrity.

Hubis and McIlroy disclose a connected state value having an attribute that is used to determine security permissions *(see above)*. Additionally, McIlroy discloses that a label is either a mathematical element or one of two special symbols, each implying either being completely accessible or completely inaccessible. Though it is possible to conceive of the data structure storing the mathematical element or special symbols being a numerical value, McIlroy does not *expressly* disclose the label being a numerical value. Therefore, Hubis and McIlroy do not *expressly* disclose the connected state being a numerical value.

Feiertag discloses an attribute used to determine security permissions being a numerical value *(Feiertag, L is the set of security levels of a system, and "<" is a relation that orders the set L, which can be seen as the functionally equivalent to a set of integers, page 58 right hand column)*.

Hubis, McIlroy and Feiertag are analogous art in that they deal with multilevel computer security. At the time of the invention it would have been obvious to utilize the formal model described in Feiertag to guarantee McIlroy's multilevel security system's correctness, which would inherently include forcing McIlroy's label to be a single element from an ordered set of security clearance elements.

The motivation for doing so would have been that the Bell and LaPadula model is very

simple and allows the designer to verify easily that the definition is consistent with intuitive

understanding of multilevel security *(Feiertag, Conclusions, page 63)*.

Therefore, it would have been obvious to modify Hubis and McIlroy's system to fit into

Feiertag's formal verification scheme by making the label a numerical value for the benefit of

simplicity of design and ease of design, to obtain the invention of <u>Claim 11</u>.

15.   As per **Claim 15**, <u>Hubis</u> discloses a computer-readable storage medium including a disk

control program for executing a method of processing information based on which input or

output from or to a disk device *(disk drive storage array, column 3 lines 62-65)* connected to a

computer *(host 1, Figure 2A)* is managed, wherein said disk control program comprises:

> code for defining the relationship of logical connection *(NURAM data structures
>
> 182, Figure 2A)* between said computer and a logical volume *(logical volume, column 10
>
> line 33)* included in said disk device or a logical area *(logical volume, column 10 line 33)*
>
> in a logical volume *(physical disc drive, column 10 line 32)* on the basis of both physical
>
> identification information *(host world wide name list 153, Figure 2B-1)* that uniquely
>
> indicates said computer connected to said disk device, and logical volume connection
>
> information *(permission column 195, Figure 2B-3)* that contains a connected state value
>
> *(permission value 195, Figure 2B-3)* concerning the connection of said computer to each
>
> logical volume included in said disk device or each logical area in each logical volume;
>
> and

> code for controlling, based on the definition, whether said computer can access a
>
> logical volume included in said disk device or a logical area a logical volume *(column 4*
>
> *lines 6-8)*,

Hubis does not disclose wherein said connected state value ranges between a minimum value and a maximum value, said maximum value signifying that said computer is fully connected, said minimum value signifying that said computer is fully disconnected, an intermediate value between said maximum value and said minimum value signifying a conditionally connected state for said computer.

McIlroy discloses a connected state value *(ceiling, section 2, paragraph 1 line 3)* concerning the connection of said computer *(process. Section 2, paragraph 1 line 3)* is specified in relation to each logical volume *(file system, section 2, paragraph 1 line 3)*, said connected state value ranging between a minimum value and a maximum value *(section 2, paragraph 2 line 1)*, said maximum value *(symbol "yes", section 2, paragraph 2 line 2)* signifying that said computer is fully connected, said minimum value *(symbol "no", section 2, paragraph 2 lines 3-4)* signifying that said computer is fully disconnected, an intermediate value *(element of a mathematical lattice, section 2, paragraph 2 line 1)* between said maximum value and said minimum value signifying a conditionally connected state *(when a process label has a higher privilege than a storage label the communication may proceed, otherwise it will not, section 1, paragraph 2 lines 2-3)* for said computer.

Hubis and McIlroy are analogous art in that they both deal with the Unix operating system *(see Hubis, column 1 lines 41-43, and McIlroy, section 1, paragraph 1 line 1)* and validating authorization to access files *(see Hubis, column 3 lines 52-59, and McIlroy, section 1, paragraph 2 lines 1-2)*. At the time of the invention it would have been obvious to one having ordinary skill in the art to implement McIlroy's secure system by adding labels to Hubis' port mapping table.

The motivation for doing so would have been that the McIlroy's system provides sound, practical security *(abstract, lines 3-5)* and uses security labels to classify information for purposes of privacy and integrity *(abstract, lines 5-7)*.

Therefore, it would have been obvious at the time of the invention to implement McIlroy's security labels on Hubis' volume management system for the benefit of practical security and for purposes of privacy and integrity.

Hubis and McIlroy disclose a connected state value having an attribute that is used to determine security permissions *(see above)*. Additionally, McIlroy discloses that a label is either a mathematical element or one of two special symbols, each implying either being completely accessible or completely inaccessible. Though it is possible to conceive of the data structure storing the mathematical element or special symbols being a numerical value, McIlroy does not *expressly* disclose the label being a numerical value. Therefore, Hubis and McIlroy do not *expressly* disclose the connected state being a numerical value.

Feiertag discloses an attribute used to determine security permissions being a numerical value *(Feiertag, L is the set of security levels of a system, and "<" is a relation that orders the set L, which can be seen as the functionally equivalent to a set of integers, page 58 right hand column)*.

Hubis, McIlroy and Feiertag are analogous art in that they deal with multilevel computer security. At the time of the invention it would have been obvious to utilize the formal model described in Feiertag to guarantee McIlroy's multilevel security system's correctness, which would inherently include forcing McIlroy's label to be a single element from an ordered set of security clearance elements.

The motivation for doing so would have been that the Bell and LaPadula model is very

simple and allows the designer to verify easily that the definition is consistent with intuitive

understanding of multilevel security *(Feiertag, Conclusions, page 63)*.

Therefore, it would have been obvious to modify Hubis and McIlroy's system to fit into

Feiertag's formal verification scheme by making the label a numerical value for the benefit of

simplicity of design and ease of design, to obtain the invention of <u>Claim 15</u>.

Claim Rejections - 35 USC ' 103 – Hubis, McIlroy, Feiertag and King

16.   **Claim 5, 7 and 12** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Hubis et al *(US Patent Number 6,343,324)*, McIlroy et al. *("Multilevel Security in the UNIX*

Tradition") and <u>Feiertag</u> et al. *("Proving Multilevel Security of a System Design")* as applied to

Claims 4, 1 and 9 respectively above, in further view of King et al *("Operating System Support*

for Virtual Machines").

17.   As per **Claim 5**, <u>Hubis</u>, <u>McIlroy</u> and <u>Feiertag</u> disclose an input/output management

system according to Claim 4, wherein

> computer identification information *(Hubis, host index 151, Figure 2B-3)*

concerning said computer is specified in said computer identification information

definition division *(Hubis, port mapping table 190, Figure 2B-3)*, and

> said input/output execution control block controls whether said computer can

access a logical area in a logical volume included in said disk device *(Hubis, column 4*

lines 6-8).

Hubis, McIlroy and Feiertag do not disclose said computer including a plurality of logical

computers, wherein computer identification information concerning each of said logical

computers is specified in said computer identification information definition division, and said

input/output execution control block controls whether each of said logical computers that share

the same physical input/output path can access a logical area in a logical volume included in

said disk device.

King discloses a computer *(computer system, section 1 paragraph 1 lines 2-3)* including

a plurality of logical computers *(virtual machines, section 1 paragraph 2 lines 5-6)*,

wherein computer identification information concerning each of said logical

computers *(host index 151, Figure 2B-3, see interpretation below)* is specified in said

computer identification information definition division, and

said input/output execution control block controls whether each of said logical

computers that share the same physical input/output path can access a logical area in a

logical volume included in said disk device *(King, figure "Type I VMM", see interpretation

below)*.

The virtual machines run inside the client computer *(King, figure "Type I VMM")* and as

said client computer's access over its physical input/output path is controlled by the input/output

execution control block, inherently so would the virtual machines. Additionally, the computer

identification associated with each of said logical computers *(host index 151, Figure 2B-3)* is

identical and is specified in said computer identification information definition division.

King and Hubis are analogous art in that they both deal with systems of multiple and

heterogeneous host computers. It would have been obvious to someone with ordinary skill in

the art to run the plurality of virtual machines taught by King on the client computer in Hubis and

McIlroy's input/output management system.

King states that virtual machines can be used to provide a software environment for

debugging operating systems that is more convenient than using a physical machine *(section 1*

paragraph 2 line 13-15) and provide a convenient interface for adding functionality *(section 1 paragraph 2 line 15-19).*

Therefore, it would have been obvious to combine the host taught by Hubis and McIlroy with the virtual machines taught by King for the benefit of debugging and conveniently adding functionality, to obtain the invention as specified in claim 5.

18.   As per **Claim 7**, Hubis, McIlroy, Feiertag and King disclose an input/output management system for managing input or output from or to a disk device connected to a computer according to Claim 1,

wherein the definition *(Hubis, port mapping table 190, Figure 2B-3)* is used to control whether each of a plurality application programs running in said computer *(King, guest applications, figure "Type I VMM")* can access a logical volume included in said disk device or a logical area in a logical volume *(Hubis, column 4 lines 6-8).*

King discloses multiple applications running in a virtual machine *(guest applications, figure "Type I VMM").* The virtual machines run inside the client computer *(King, figure "Type I VMM")* and as said client computer's access over its physical input/output path is controlled by the input/output execution control block, inherently so would the virtual machines.

19.   As per **Claim 12**, Hubis, McIlroy, Feiertag and King disclose an input/output management method according to Claim 9,

wherein whether each of a plurality of application programs running in said computer *(King, guest applications, figure "Type I VMM")* can access a logical volume included in said disk device or a logical area in a logical volume is controlled *(Hubis, column 4 lines 6-8).*

Claim Rejections - 35 USC ' 103 – Hubis, McIlroy, Feiertag and Tang

20.   **Claim 13** is rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Hubis</u> et al *(US Patent Number 6,343,324)*, <u>McIlroy</u> et al. *("Multilevel Security in the UNIX Tradition")* and <u>Feiertag</u> et al. *("Proving Multilevel Security of a System Design")* as applied to <u>Claim 11</u> above, in further view of <u>Tang</u> et al *("Load Distribution via Static Scheduling and Client Redirection for Replicated Web Servers")*.

21.   As per **Claim 13**, <u>Hubis</u>, <u>McIlroy</u> and <u>Feiertag</u> disclose an input/output management method according to Claim 11, wherein a plurality of pieces of definition information *(port mapping table entry 191, Figure 2B-3)* define whether said computer or each of a plurality of application programs running in said computer can access a logical volume included in said disk device or a logical area in a logical volume *(column 4 lines 6-8)*. Hubis and McIlroy do not disclose the plurality as being automatically switched with the start of each of time zones according to a predefined schedule.

The limitation *"said computer or each of a plurality of application programs running in said computer"* can be fulfilled by one or more of the limitations *"said computer"* or *"each of a plurality of application programs running in said computer"*.

Tang discloses a plurality of pieces of definition information as being automatically switched *(section 2 item 2 lines 3-5)* with the start of each of time zones *(period of T_s, section 2 item 2 line 3)* according to a predefined schedule *(section 2 item 2)*.

Hubis and Tang are analogous art in that they deal with managing the connection relationship between clients accessing data from one of a plurality of storage locations. It would have been obvious to someone with ordinary skill in the art to schedule connections in Hubis and McIlroy's storage system with Tang's scheduler.

Tang discloses that using a scheduler allows user-specific data to be migrated or located at a specific storage location *(section 1 paragraph 3 lines 11-13)* while still keeping the load on each storage location balanced *(section 1 paragraph 3 lines 13-14)*.

Therefore, it would have been obvious to combine the storage system taught by Hubis and McIlroy with the scheduler taught by Tang for the benefit of minimizing data replication and balancing the load on each storage location, to obtain the invention as specified in Claim 13.

Though not required for the current rejection, the Examiner notes that as per the rejection of Claim 7, King *("Operating System Support for Virtual Machines")* discloses a computer *(computer system, section 1 paragraph 1 lines 2-3)* including a plurality of applications *(guest applications, figure "Type I VMM")*.

Claim Rejections - 35 USC ' 103 – Hubis, McIlroy, Feiertag, King and Tang

22.   **Claims 8** is rejected under 35 U.S.C. 103(a) as being unpatentable over Hubis et al *(US Patent Number 6,343,324)*, McIlroy et al. *("Multilevel Security in the UNIX Tradition")*, Feiertag et al. *("Proving Multilevel Security of a System Design")* and King et al *("Operating System Support for Virtual Machines")* as applied to Claim 7 above, and in further view of Tang et al *("Load Distribution via Static Scheduling and Client Redirection for Replicated Web Servers")*.

23.   As per **Claim 8**, Hubis, McIlroy, Feiertag and King disclose an input/output management system according to Claim 7, wherein

a plurality of pieces of computer identification information *(Hubis, port mapping table entry 191, Figure 2B-3)* defining whether said computer or each of said application programs *(King, guest applications, figure "Type I VMM")* can access a logical volume included in said disk device or a logical area in a logical volume *(Hubis, col. 4 lines 6-8)*.

Hubis, McIlroy and King do not expressly disclose the system further comprising a schedule definition division containing said plurality of pieces of computer identification information being specified in relation to respective time zones, and in which a schedule for automatically changing the plurality of pieces of computer identification information is predefined.

Tang discloses a system comprising a schedule definition division containing a plurality of pieces of computer identification information (hostname/IP address, section 2.1 line 3) being specified in relation to respective time zones (period of T_s, section 2 item 2 line 3), and in which a schedule for automatically changing the plurality of pieces of computer identification information is predefined (section 2 item 2).

Regarding the limitation "a schedule definition division", Tang discloses a scheduler generating and storing assignments between client networks and assigned servers (section 2.2 lines 1-2). Although not expressly mentioned, it is inherent in the storing operation for the scheduler to store the assignments in an accessible way in memory. Assignments stored in an accessible way in memory can be considered a data structure, and this data structure subsequently fulfils the limitation of a schedule definition division.

Hubis, McIlroy, King and Tang are analogous art in that they deal with managing the connection relationship between clients accessing data from one of a plurality of storage locations. It would have been obvious to someone with ordinary skill in the art to schedule connections in Hubis and King's storage system with Tang's scheduler.

Tang discloses that using a scheduler allows user-specific data to be migrated or located at a specific storage location (section 1 paragraph 3 lines 11-13) while still keeping the load on each storage location balanced (section 1 paragraph 3 lines 13-14).

Therefore, it would have been obvious to combine the storage system taught by Hubis,

McIlroy and King with the scheduler taught by Tang for the benefit of minimizing data replication

and balancing the load on each storage location, to obtain the invention as specified in Claim 8.

Claim Rejections - 35 USC ' 103 – Hubis, McIlroy, Feiertag and Reynolds

24.   **Claim 14** is rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Hubis</u> et al *(US*

Patent Number 6,343,324), <u>McIlroy</u> et al. *("Multilevel Security in the UNIX Tradition")* and

<u>Feiertag</u> et al. *("Proving Multilevel Security of a System Design")* as applied to <u>Claim 10</u> above,

and in further view of <u>Reynolds</u> et al *("The Design and Implementation of an Intrusion Tolerant*

System").

25.   As per **Claim 14**, <u>Hubis</u>, <u>McIlroy</u> and <u>Feiertag</u> disclose the input/output management

method according to <u>Claim 10</u>, including definition information *(Hubis, NURAM data structures*

182, Figure 2A) that defines whether said computer or each of a plurality of application

programs running in said computer can access a logical volume included in said disk device or

a logical area in a logical volume *(column 4 lines 6-8)*. Hubis and McIlroy do not expressly

disclose the definition information being automatically modified with a system failure occurring in

said connected computer as a trigger.

The limitation *"said computer or each of a plurality of application programs running in*

said computer" can be fulfilled by one or more of the limitations *"said computer"* or *"each of a*

plurality of application programs running in said computer".

<u>Reynolds</u> discloses a system wherein a computer's access is automatically modified with

a system failure *(page 4 column 1 lines 7-11)* occurring in said connected computer as a trigger

(page 4 column 1 lines 33-35).

Hubis and Reynolds are analogous art in that they both deal with the way clients access

servers. It would have been obvious to one with ordinary skill in the art to combine Hubis'

storage system with Reynolds failure detection system. Reynolds discloses that fault tolerant

techniques usually are designed to work against faults *(page 1 column 2 lines 4-5)*. Reynolds

also states that faults produce vulnerabilities that can be exploited by an attacker *(page 1*

column 2 lines 8-10).

Therefore, it would have been obvious to combine the storage system taught by Hubis

and McIlroy with the fault detection taught by Reynolds for the benefit of protection against

vulnerabilities, to obtain the invention as specified in claim 14.

Though not required for the current rejection, the Examiner notes that as per the

rejection of Claim 7, King *("Operating System Support for Virtual Machines")* discloses a

computer *(computer system, section 1 paragraph 1 lines 2-3)* including a plurality of applications

(King, guest applications, figure "Type I VMM").

Claim Rejections - 35 USC ' 103 – Hubis, McIlroy, Feiertag and Mullen

26.   **Claims 16-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Hubis</u> et

al *(US Patent Number 6,343,324)*, <u>McIlroy</u> et al. *("Multilevel Security in the UNIX Tradition")* and

<u>Feiertag</u> et al. *("Proving Multilevel Security of a System Design")* as applied to <u>Claim 10</u> above,

and in further view of <u>Mullen</u> *("Restrict Anonymous: Enumeration and the Null User")*.

27.   As per **Claims 16 and 17**, <u>Hubis</u>, <u>McIlroy</u> and <u>Feiertag</u> disclose an input/output

management system according to Claims 1 and 2 respectively above, wherein if said connected

state value is an intermediate value, then:

> an access key *(label, section 1, paragraph 2 line 1)* is appended *(the label is*
>
> *inherently appended to a process in that the IX system is a modification of a UNIX*

system where one of the modifications was to add the element "label" to the filesystem,

section 7.3) to an input/output request *(process, section 1, paragraph 2 line 1)* issued by

said computer;

if said access key is larger than said connected state value *(section 2.1,*

paragraph 1 lines 2-3), input/output for said input/output request is disabled *(requirement*

not held -> data may not flow, section 2.1, paragraph 1 lines 2-3); and

if said access key is equal to or smaller than said connected state value *(section*

2.1, paragraph 1 lines 2-3), input/output for said input/output request is enabled

(requirement held -> data may flow, section 2.1, paragraph 1 lines 2-3).

Hubis, McIlroy and Feiertag do not disclose that if an access key is not appended to an

input/output request issued by said computer, said computer is treated as fully disconnected.

<u>Mullen</u> discloses that if an access key is not appended to an input/output request issued

by said computer *(a user account exists that does not have credentials, paragraph 2 ("Before*

we...") lines 9-11), said computer is treated as fully disconnected *(paragraph 5 ("This*

obviously...") lines 1-7).

Hubis, McIlroy and Feiertag and Mullen are analogous art in that they deal with checking

credentials on a networked system. At the time of the invention it would have been obvious to

one with ordinary skill in the art to block the connection of one of Hubis and McIlroy's hosts if it

does not have a label, as taught by Mullen.

Mullen teaches that by not having credentials, a user account can do things that would

not be allowed if it had proper credentials and can be used to glean a tremendous amount of

information from a network without raising any eyebrows *(paragraph 2, lines 9-11).*

Therefore, it would have been obvious to combine Hubis and McIlroy's secure connection system with Mullen's insight about not having credentials for the benefit of securing the system to obtain the invention as specified in Claims 16 and 17.

28.   As per **Claims 18 and 19**, Hubis, McIlroy and Feiertag disclose an input/output management method according to Claims 9 and 11 respectively above, wherein if said connected state value is an intermediate value, then:

an access key *(label, section 1, paragraph 2 line 1)* is appended *(the label is inherently appended to a process in that the IX system is a modification of a UNIX system where one of the modifications was to add the element "label" to the filesystem, section 7.3)* to an input/output request *(process, section 1, paragraph 2 line 1)* issued by said computer;

if said access key is larger than said connected state value *(section 2.1, paragraph 1 lines 2-3)*, input/output for said input/output request is disabled *(requirement not held -> data may not flow, section 2.1, paragraph 1 lines 2-3)*; and

if said access key is equal to or smaller than said connected state value *(section 2.1, paragraph 1 lines 2-3)*, input/output for said input/output request is enabled *(requirement held -> data may flow, section 2.1, paragraph 1 lines 2-3)*.

Hubis and McIlroy do not disclose that if an access key is not appended to an input/output request issued by said computer, said computer is treated as fully disconnected.

Mullen discloses that if an access key is not appended to an input/output request issued by said computer *(a user account exists that does not have credentials, paragraph 2 ("Before we...") lines 9-11)*, said computer is treated as fully disconnected *(paragraph 5 ("This obviously...") lines 1-7)*.

Hubis, McIlroy and Mullen are analogous art in that they deal with checking credentials on a networked system. At the time of the invention it would have been obvious to one with ordinary skill in the art to block the connection of one of Hubis and McIlroy's hosts if it does not have a label, as taught by Mullen.

Mullen teaches that by not having credentials, a user account can do things that would not be allowed if it had proper credentials and can be used to glean a tremendous amount of information from a network without raising any eyebrows *(paragraph 2, lines 9-11)*.

Therefore, it would have been obvious to combine Hubis and McIlroy's secure connection system with Mullen's insight about not having credentials for the benefit of securing the system to obtain the invention as specified in Claims 18 and 19.

29.   As per **Claim 20**, Hubis, McIlroy and Feiertag disclose a computer-readable storage medium according to Claim 15, wherein if said connected state value is an intermediate value, then:

an access key *(label, section 1, paragraph 2 line 1)* is appended *(the label is inherently appended to a process in that the IX system is a modification of a UNIX system where one of the modifications was to add the element "label" to the filesystem, section 7.3)* to an input/output request *(process, section 1, paragraph 2 line 1)* issued by said computer;

if said access key is larger than said connected state value *(section 2.1, paragraph 1 lines 2-3)*, input/output for said input/output request is disabled *(requirement not held -> data may not flow, section 2.1, paragraph 1 lines 2-3)*; and

if said access key is equal to or smaller than said connected state value *(section 2.1, paragraph 1 lines 2-3)*, input/output for said input/output request is enabled *(requirement held -> data may flow, section 2.1, paragraph 1 lines 2-3)*.

Hubis and McIlroy do not disclose that if an access key is not appended to an input/output request issued by said computer, said computer is treated as fully disconnected.

Mullen discloses that if an access key is not appended to an input/output request issued by said computer *(a user account exists that does not have credentials, paragraph 2 ("Before we...") lines 9-11)*, said computer is treated as fully disconnected *(paragraph 5 ("This obviously...") lines 1-7)*.

Hubis, McIlroy and Mullen are analogous art in that they deal with checking credentials on a networked system. At the time of the invention it would have been obvious to one with ordinary skill in the art to block the connection of one of Hubis and McIlroy's hosts if it does not have a label, as taught by Mullen.

Mullen teaches that by not having credentials, a user account can do things that would not be allowed if it had proper credentials and can be used to glean a tremendous amount of information from a network without raising any eyebrows *(paragraph 2, lines 9-11)*.

Therefore, it would have been obvious to combine Hubis and McIlroy's secure connection system with Mullen's insight about not having credentials for the benefit of securing the system to obtain the invention as specified in Claim 20.

III. CLOSING COMMENTS

30.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office Action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP ' 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

a. STATUS OF CLAIMS IN THE APPLICATION

31.   The following is a summary of the treatment and status of all claims in the application as recommended by M.P.E.P. ' 707.07(i):

A(1). CLAIMS REJECTED IN THE APPLICATION

32.   Per the instant office action, Claims 1-20 have received an action on the merits and are

subject of a final action.

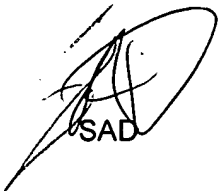### b. DIRECTION OF FUTURE CORRESPONDENCES

33.   Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Sam Dillon whose telephone number is 571- 272-8010. The examiner can

normally be reached on 9:30-6:00.

34.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Sanjiv Shah can be reached on 571-272-4098. The fax phone number for the

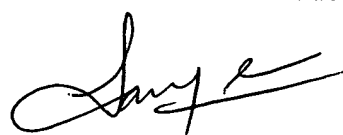organization where this application or proceeding is assigned is 571-273-8300.

IMPORTANT NOTE

35.   Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you

would like assistance from a USPTO Customer Service Representative or access to the

automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sam Dillon
Examiner
Art Unit 2185

SANJIV SHAH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100